



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/356,940	07/19/1999	JOSEPH GRAJEWSKI	438P470	8491

7590 07/09/2003

GEORGE R MCGUIRE  
HANCOCK & ESTABROOK  
1500 MONY TOWER I  
P O BOX 4976  
SYRACUSE, NY 132214976

EXAMINER
----------

WERNER, BRIAN P

ART UNIT	PAPER NUMBER
----------	--------------

2621

DATE MAILED: 07/09/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/356,940	GRAJEWSKI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Brian P. Werner	2621	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 25 April 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 33-54 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 33-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                  | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 25, 2003 has been entered.

### ***Response to Amendment***

2. The amendment with remarks filed on April 25, 2003 has been entered. Claims 33-54 remain pending, with claims 37, 43, 49, 51 and 53 currently amended. In responsive, the previous objection to claims 37 and 49 is withdrawn, and the 112 rejections of claims 43, 44, 51, 52 and 53 are withdrawn.

***Response to Arguments***

3. Each of the remarks and/or arguments filed with the aforementioned amendment have been considered:

Claim Objections:

Summary of Remarks: The previously objected to claims have been amended.

Examiner's Response: The objections are withdrawn.

Claim 112 rejections:

Summary of Remarks: The previously rejected claims under 112 have been amended.

Examiner's Response: The 112 rejections are withdrawn.

Claims 45 and 53 rejected under 35 U.S.C. 103(a) as being unpatentable over the examiner's own experience, in view of In re Venner (262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958))

Summary of Remarks: Applicant disagrees with the rejection, providing an interpretation of In re Venner and citing various other case law.

Examiner's Response: The examiner disagrees with applicant's assessment of In re Venner and the associated case law cited, and the examiner maintains that the claims merely automate (or place into an automated environment) what people have been doing manually for decades as described in the previous Office Action. However,

Art Unit: 2621

because the prior art (including the newly cited art) so clearly teaches every element of the claims as described herein, and in order to expedite prosecution, this ground of rejection is withdrawn in favor of the prior art.

Claims 45-48 and 53 rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and He (US 5,944,824 A)

Summary of Remarks: "Each and every element of the claimed invention must be disclosed by the combination of references" (beginning at response page 10, bottom line).

Examiner's Response: Examiner agrees. Each and every claim element of claims 33-54 is taught by the prior art of record, as well as the newly cited prior art, as described in the rejections and response to arguments below.

Summary of Remarks: "There must be a suggestion or motivation in the references themselves or the knowledge of one skilled in the art to make the proposed combination" (response page 11, top paragraph).

Examiner's Response: Examiner agrees. Motivation for the prior art combinations was advanced in the previous Office Action and in the rejections below, as well as addressed by the examiner in the response to remarks below.

Summary of Remarks: "The proposed combination of references does not disclose the claimed circuitry for randomly generating a password that is uniquely associated with each indicia stored in the device" (response page 11, top paragraph).

Examiner's Response: Examiner disagrees. First, this remark appears to directed to prior art not teaching each and every claimed element, and not to the propriety of the combination per se. Thus, the McIntosh and He references individually "discloses" both randomly generating a password and uniquely associating each password with each indicia stored in the device as follows:

- "The claimed circuitry for randomly generating a password" is disclosed by He ("user password may be randomly set" at column 7, line 58); and
- "a password that is uniquely associated with each indicia stored in the device" is disclosed by McIntosh (McIntosh generates a password as, for example, a "sequence of numbers" at page 2, line 45; the indicia "BC" is uniquely associated in the memory 40 of the device 5 with the password of, for example "1234" at page 3, line 42 for subsequent recall and display to the user).

Thus, the individual references teach each and every claimed element. Regarding the "combination" of references, the examiner states in the rejection below that (in part):

Art Unit: 2621

"It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the password circuitry of McIntosh according to the teaching of He, by including a random number generator to generate random passwords/PINs for the user for purposes of gaining access to his/her secure accounts so that when it comes time for the user to either choose a password, or to change a password, the password can be randomly generated ..."

The individual references not only teach each and every claimed element, but the combination is properly founded.

Summary of Remarks: "McIntosh does not disclose the generation of random passwords" (response page 11, first paragraph).

Examiner's Response: Yes and no. McIntosh does disclose the random generation of incorrect passwords at page 4, lines 22-27. However, McIntosh does not disclose the random generation of actual passwords for unique association with the indicia as required by the claims. Thus, the He reference is relied upon as described in detail in the response to remarks below.

Summary of Remarks: "He creates a random password" (Response page 11, bottom paragraph).

Examiner's Response: Examiner agrees.

Summary of Remarks: He lacks "the random generation of a password for unique association with stored indicia representing a secured site" (Response page 11, bottom paragraph).

Art Unit: 2621

Examiner's Response: The He reference is not relied upon solely as teaching the random generation of a password for unique association with stored indicia representing a secured site. Looking at the actual rejection both in the previous Office Action and herein, the He reference is relied upon as "teaching". Specifically, the He reference teaches the random generation of a user password for access to a secure system. It is McIntosh that teaches the unique association of a user's own password, whether randomly generated by the user or not, with an indicia. Together, as part of the McIntosh and He combination, all of these elements are taught.

Summary of Remarks: "It is unclear how a combination of He and McIntosh is even possible, as one reference involves a security system for a portable ATM pin memory device while the other relates to improving user accessibility by normalizing security operations across an entire computer network environment" (response page 12, top paragraph).

Examiner's Response: The combination is very simple, and very possible. McIntosh discloses a portable device for storing and associating indicia with passwords. The passwords of McIntosh are a user's passwords, where the user may enter an existing password that is associated with an indicia or, in the case when the user is opening new account or changing an existing password, the user may enter a password that is made up on the spot. McIntosh anticipates all of this. The He reference is relied upon as a **TEACHING** of randomly generating a user's password with **MOTIVATION** for doing so. The entire He reference, including improving user accessibility by normalizing



Art Unit: 2621

security operations across an entire computer network environment as argued by applicant, is neither relied upon by the examiner, nor bodily incorporated into the McIntosh reference. The test for obviousness is not whether the features of the He reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or both of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Regarding applicant's question of "how a combination of He and McIntosh is even possible", it's very simple:

***Modify the random password generator already disclosed by McIntosh to randomly generate a password for a user as taught by He, should the user desire one.***

The motivation for doing so is:

***To "increase the security level due to the unpredictability of the password" (He, column 8, line 1) and "for convenience and for uniqueness" (He, column 13, line 6), thus ensuring a completely random password not influenced by the knowledge of the user and thus making it more difficult for a hacker to predict or figure out the user's password, and for convenience.***

Summary of Remarks: "It is insufficient that both references are in the same general field of art or even that they may be combined. See MPEP § 2143.01 (citing *In re Mills* ...) (response page 12, top paragraph).

Examiner's Response: MPEP § 2143.01, under the section that discusses *In re Mills*, states (in part, with emphasis added):

"The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also ***suggests the desirability of the combination***" and

"... must be a ***suggestion or motivation in the reference*** to do so"

However, this portion of the MPEP should not be read or interpreted in a vacuum.

MPEP 2143.01 also state that (in part, with emphasis added):

"Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some ***teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art.***"

Therefore, the motivation or suggestion to combine may be explicit, implicit, or generally available to one of ordinary skill in the art. In the case of the McIntosh and He combination, while the motivation advanced by the examiner meets all three criteria, it certainly meets the most compelling criteria of "explicit". In the rejection advanced below (and in the previous Office Action), the motivation is stated as follows:

Art Unit: 2621

"The above combination would serve to "increase the security level due to the unpredictability of the password" (He, column 8, line 1) and "for convenience and for uniqueness" (He, column 13, line 6), thus ensuring a completely random password not influenced by the knowledge of the user and thus making it more difficult for a hacker to predict or figure out the user's password, and for convenience."

Thus, to answer the question of why one of ordinary skill in the art would want to modify McIntosh according to the teaching of He, ***the answer lies in the explicit words of the He reference***. That is, for:

Unpredictability

Uniqueness

Convenience

Difficulty in hacking

Summary of Remarks: "In fact, the references cannot be combined, as to do so would frustrate the sole purpose of McIntosh ... the device would never provide the proper ATM pin numbers and a user would never be able to access his bank account because the pin number generated by the device and provided to the user would not match the pin number that the bank has already assigned to the account" (response page 12, top paragraph).

Examiner's response: Not true. The "sole purpose" of the McIntosh system is to store indicia (e.g., account names) with associated passwords so that the user may conveniently recall them when necessary. McIntosh is not so much concerned with how

Art Unit: 2621

the user generates the passwords to begin with. In the combination as described above, the user would be provide with the option of, upon entry of an indicia, having the password randomly generated instead of generating one himself. Often times, when accounts are opened, a user must decide upon a password himself. This knowledge is generally available not only to one of ordinary skill, but to everybody. Other times, a user might be prompted to change a password. This knowledge is also generally available. In the McIntosh and He combination, the password could be decided randomly for the reasons and motivation cited by He. The applicant's remarks that "the device would never provide the proper ATM pin numbers and a user would never be able to access his bank account because the pin number generated by the device and provided to the user would not match the pin number that the bank has already assigned to the account" misconstrues the McIntosh and He combination. The applicant is assuming that even for existing accounts having existing passwords, the combination would generate new random passwords. This is not the case. In the combination, the ability of the McIntosh to generate random passwords is present if the user decides to do so. ***The teaching of He as relied upon by the examiner is that upon deciding upon a password for a secure system, randomly generated password is more secure, less prone to hacking, and more convenient to a user. It is this teaching that is relied upon by the examiner, and not the entire He reference.***

Summary of Remarks: The examiner "failed to identify a proper motivation or suggestion to make the proposed combination" (response page 12, bottom paragraph).

Examiner's Response: The motivation is addressed above.

Summary of Remarks: The examiner "did not explain how He motivates the proposed modification of the portable storage device in McIntosh to assign random passwords to associated indicia as claimed in the application" (response page 12, bottom paragraph).

Examiner's Response: The combination and motivation for making the combination is addressed above.

Summary of Remarks: "The references do not disclose each limitation recited in claim 45 as they do not teach the claimed association of passwords with indicia, nor do they contain a motivation to assign unique passwords to each such indicia" (response page 13, top paragraph).

Examiner's Response: The combination and motivation for making the combination is addressed above.

Summary of Remarks: The combination is "based on improper hindsight analysis" (response page 13, top paragraph).

Examiner's Response: Any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account

Art Unit: 2621

only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). The combination is proper, with motivation for making the combination taken directly from the references as addressed above.

The Remainder of the Arguments:

The remainder of the arguments at response pages 13, second paragraph through response page 14 are all based on the McIntosh and He combination, and those arguments have been addressed above.

In response to the applicant's remarks regarding the McIntosh and He references individually and in combination, the new rejections advanced herein are provided to demonstrate that the invention, as currently claimed, would have been obvious to one of ordinary skill in the art.

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 38-52 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

All pending claims are not original. Independent claims 33 and 45 recite a method of associating a plurality of random numbers with indicia that is not supported by the original disclosure (i.e., specification, claims, abstract and drawings).

Independent claim 33 will be used to exemplify the non-supported subject matter.

Given that independent claim 45 recites equivalent non-supported subject matter, it too is rejected on the same grounds. Claims 34-44 and 46-52 are rejected as depending from these claims.

Independent claim 33, at steps g and h, recites (in part, with emphasis added):

... permitting said individual to store in said data storage source a ***plurality of indicia*** each one of which is representative of a secured site; and

password circuitry for generating a plurality of passwords, wherein each of said ***plurality of passwords is uniquely associated with a respective one of said plurality of indicia.***"

The scope of these claim elements cover the storage of a plurality of indicia before the generation of any passwords. Then, after the plural indicia are stored, the passwords are generated. Following the generation of the passwords, they are then associated with the indicia all at once. However, the specification and original disclosure describes a process of storing a single indicia, generating a single password, and then associating that single password with that indicia. While, according to the original disclosure, the process can be repeated for additional indicia one at a time (i.e., in series; refer to specification page 7, top paragraph), the original disclosure does not support associating plural passwords with plural indicia all at once (i.e., in parallel).

Independent claim 45 recites equivalent limitations at steps c and d.

Note that independent claim 53 is not rejected because step d requires the steps of associating a password with an indicia is performed "in sequence" at step d. This is supported by the original disclosure.



***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 45-48 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and He (US 5,944,824 A).

McIntosh:

Regarding claims 45 and equivalent claim 53, McIntosh discloses:

a portable body member (figure 1, numeral 5);

a data storage in the body (figure 2, numeral 40);

a user interface and communication components (figure 1, numerals 10, 15, 20 and 25) permitting an individual to store plural indicia representative of a secure site in the storage ("letters" at page 2, line 44; e.g., "BC" at page 3, line 39); and

password circuitry for allowing a user to generate a plurality of random passwords, wherein each password is uniquely associated with a respective one of the indicia ("sequence of numbers" at page 2, line 45; e.g., "1234" at page 3, line 42; in the example given by McIntosh at page 3, lines 25-44, the indicia "BC" is uniquely associated with the password "1234"; the input keys, along with their control circuitry and the memory 40, is circuitry that allows for the generation of passwords by a user;

Art Unit: 2621

McIntosh anticipates the generation of random passwords, as the user may enter any password desired; even in the example at page 3, the password exemplified is "say 1234" at line 42, which is random).

Regarding claim 53 specifically, the steps of associating a password with an indicia can be repeated by a user as many times as desired as permitted by the memory capacity of the memory device ("... entered and recorded in like manner if so desired" at page 4, line 1).

Regarding claim 46, indicia selection circuitry is disclosed (figure 4, "punch in account designation").

Regarding claim 47, recall circuitry is disclosed (figure 4, "pin number").

Regarding claim 48, a display is disclosed (figure 1, numeral 15).

Differences:

While McIntosh uniquely associates a user-entered random password with a respective one of the indicia, and while McIntosh teaches a random number generator for purposes other than generating actual passwords (i.e., "unit 55 capable of generating a random sequence of numbers when required" at page 3, line 14), McIntosh does not disclose "password circuitry comprising a random number generator for randomly generating a plurality of passwords".

He:

Art Unit: 2621

He discloses a password protected secure system, where a user identifier is associated with a password ("user identifier and a password" at column 5, line 8), comprising a random number generator (figure 7, numeral 148) for randomly generating a password for a use to gain access to the system ("the selection of a password may be randomly determined" at column 7, line 58; "random selection of the password" at column 7, line 67).

Obviousness Statement:

It would have been obvious at the time the invention was made to one of ordinary skill in the art to add a random password generating circuit, or to modify the password circuitry already disclosed by McIntosh according to the teaching of He, to generate a random passwords/PIN for the user for purposes of gaining access to his/her secure accounts so that when it comes time for the user to either choose a password, or to change a password, the password can be randomly generated. The above combination would serve to "increase the security level due to the unpredictability of the password" (He, column 8, line 1) and "for convenience and for uniqueness" (He, column 13, line 6), thus ensuring a completely random password not influenced by the knowledge of the user and thus making it more difficult for a hacker to predict or figure out the user's password, and for convenience.

Art Unit: 2621

8. Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and He (US 5,944,824 A) as applied to claim 47 above, and further in view of Bang (US 6,088,143 A).

The McIntosh and He combination does not teach a communication port on the portable device for directly transmitting the password(s) to the secure site(s).

Bang teaches a remote password key system ("infrared password key system" at column 1, line 19) comprising a communication port ("infrared transmitter" at column 3, line 29) for directly transmitting a password ("the password signal directed for direct transmittal" at column 3, line 31) to a secure site ("transmitting ... to the computer" at column 3, line 33).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to provide the portable device of the McIntosh and He combination, with a direct password transmission port as taught by Bang, in order to "simplify the computer password input procedure and to reduce the possibility of unintentional password disclosure to a third party when entering a password" (Bang, column 1, line 20).

9. Claims 50-52 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and He (US 5,944,824 A) as applied to claim 45 above, and further in view of Guthrie et al. (US 6,161,185 A).

Regarding claim 50, the McIntosh and He combination does not teach prompting the user to change a password after expiration of a predetermined period of time.

Regarding claim 51, the combination does not teach clock circuitry and circuitry to display a message requiring the individual to reply to continue using the device.

Regarding claim 50, Guthrie discloses a personal authentication system comprising prompting the user to change a password ("requiring users to change their passwords" and "sufficient notice" at column 2, lines 35 and 36) after expiration of a predetermined period of time ("expire after a predetermined period of time" at column 2, line 34).

Regarding claim 51, Guthrie teaches clock circuitry (i.e., the circuitry that keeps track of the time period as described above) and circuitry to display a message requiring the individual to reply (i.e., the aforementioned circuitry that provides "sufficient notice") to continue using the device ("locked out" at column 2, line 39).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the McIntosh and He combination, to notify and require the user to change passwords associated with the indicia after predetermined periods of time, in order to "foil a malicious user's attempt at 'hammering' the authentication system with responses attempting to stumble upon a correct password to gain access" (Guthrie, column 2, line 53).

Regarding claim 51, the combination does not teach generating a new password when the prompt is actuated. However, in the above McIntosh, He and Guthrie combination, it would have been obvious to allow the user to change his password in response to the prompt taught by Guthrie, by randomly generating another password in

Art Unit: 2621

accordance with the McIntosh and He combination, so as to ensure that the user is not locked out.

Regarding claim 54, the limitations therein are met by the McIntosh, He and Guthrie combination as described above.

10. Claims 33-36, 38, 39, 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and He (US 5,944,824 A) as applied to claim 45-48 and 53 above, and further in view of Ramachandran (US 6,315,195 B1).

The elements of claims 33-36, 38 and 39 (other than the differences discussed below) are met by the McIntosh and He combination as described in the rejections above. Regarding claim 40 specifically, McIntosh teaches that a preselected string of predetermined length is stored ("first four letters" and "remaining two letters" at page 3, line 30).

The McIntosh and He combination requires an initial password be entered for a user to gain access to the accounts and associated passwords stored therein (e.g., "the password" and "FLAG" at page 3, lines 32 and 33). The McIntosh and He combination does not teach using biometrics for this same purpose. Specifically, the combination does not teach a biometric interface engaged with the body, a non-volatile memory, generating and storing an initialized biometric template and comparing with a second generated biometric template upon subsequent presentation for enabling the device.

Ramachandran discloses a portable device (e.g., figures 1 and 2) for storing pin numbers (e.g., figures 82+) as described fully in the previous Office Action, comprising biometric interface engaged with the body (figure 4, numeral 47), a non-volatile memory (figure 4, numeral 38), generating and storing an initialized biometric template ("data representative of the identifying biometric features" at column 8, line 59) and comparing with a second generated biometric template upon subsequent presentation ("compare" at column 12, line 24) for enabling the device ("enable authorized users of the card" at column 8, line 61). Regarding claim 39 specifically, a fingerprint reader is disclosed ("fingerprint" at column 8, line 53).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to replace the initial password circuitry of the McIntosh and He combination, with biometrics comparison circuitry as taught by Ramachandran as described above, in order to "increase the security level" (Ramachandran, column 11, line 8) thus providing increased protection from an unauthorized user from gaining access to the legitimate user's passwords.

Regarding claim 41, while the McIntosh and He combination teaches a plurality of function keys on the portable device (i.e., McIntosh, figure 1, numeral 10), arrow keys are not disclosed. However, McIntosh states that "a more complex version of the device 5 might well be produced incorporating ... more function keys" at page 4, line 33. Ramachandran discloses arrow keys (figure 1, numerals 4 and 26) for purposes of scrolling up and down through a data list. It would have been obvious at the time the invention was made to one of ordinary skill in the art to provide the arrow keys of

Ramachandran, on the device of the McIntosh and He combination, to increase functionality as suggested by McIntosh, and to allow a user to scroll through a list of data without having to re-enter the initial password each time.

11. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A), He (US 5,944,824 A) and Ramachandran (US 6,315,195 B1) as applied to claim 35 above, and further in view of Bang (US 6,088,143 A).

The McIntosh, He and Ramachandran combination does not teach a communication port on the portable device for directly transmitting the password(s) to the secure site(s).

Bang teaches a remote password key system ("infrared password key system" at column 1, line 19) comprising a communication port ("infrared transmitter" at column 3, line 29) for directly transmitting a password ("the password signal directed for direct transmittal" at column 3, line 31) to a secure site ("transmitting ... to the computer" at column 3, line 33).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to provide the portable device of the McIntosh, He and Ramachandran combination, with a direct password transmission port as taught by Bang, in order to "simplify the computer password input procedure and to reduce the possibility of unintentional password disclosure to a third party when entering a password" (Bang, column 1, line 20).



Art Unit: 2621

12. Claims 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A), He (US 5,944,824 A) and Ramachandran (US 6,315,195 B1) as applied to claim 33 above, and further in view of Guthrie et al. (US 6,161,185 A).

Regarding claim 42, the McIntosh, He and Ramachandran combination does not teach prompting the user to change a password after expiration of a predetermined period of time.

Regarding claim 43, the combination does not teach clock circuitry and circuitry to display a message requiring the individual to reply to continue using the device.

Regarding claim 42, Guthrie discloses a personal authentication system comprising prompting the user to change a password ("requiring users to change their passwords" and "sufficient notice" at column 2, lines 35 and 36) after expiration of a predetermined period of time ("expire after a predetermined period of time" at column 2, line 34).

Regarding claim 43, Guthrie teaches clock circuitry (i.e., the circuitry that keeps track of the time period as described above) and circuitry to display a message requiring the individual to reply (i.e., the aforementioned circuitry that provides "sufficient notice") to continue using the device ("locked out" at column 2, line 39).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the McIntosh, He and Ramachandran combination, to notify and require the user to change passwords associated with the indicia after predetermined periods of time, in order to "foil a malicious user's attempt at 'hammering' the

Art Unit: 2621

authentication system with responses attempting to stumble upon a correct password to gain access" (Guthrie, column 2, line 53).

Regarding claim 44, the combination does not teach generating a new password when the prompt is actuated. However, in the above McIntosh, He, Ramachandran and Guthrie combination, it would have been obvious to allow the user to change his password in response to the prompt taught by Guthrie, by randomly generating another password in accordance with the McIntosh and He combination, so as to ensure that the user is not locked out.

13. Claims 45-48 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and Noll et al. (US 5,732,138 A).

McIntosh:

Regarding claims 45 and equivalent claim 53, McIntosh discloses:

a portable body member (figure 1, numeral 5);

a data storage in the body (figure 2, numeral 40);

a user interface and communication components (figure 1, numerals 10, 15, 20 and 25) permitting an individual to store plural indicia representative of a secure site in the storage ("letters" at page 2, line 44; e.g., "BC" at page 3, line 39); and

password circuitry for allowing a user to generate a plurality of random passwords, wherein each password is uniquely associated with a respective one of the indicia ("sequence of numbers" at page 2, line 45; e.g., "1234" at page 3, line 42; in the

Art Unit: 2621

example given by McIntosh at page 3, lines 25-44, the indicia "BC" is uniquely associated with the password "1234"; the input keys, along with their control circuitry and the memory 40, is circuitry that allows for the generation of passwords by a user; McIntosh anticipates the generation of random passwords, as the user may enter any password desired; even in the example at page 3, the password exemplified is "say 1234" at line 42, which is random).

Regarding claim 53 specifically, the steps of associating a password with an indicia can be repeated by a user as many times as desired as permitted by the memory capacity of the memory device ("... entered and recorded in like manner if so desired" at page 4, line 1).

Regarding claim 46, indicia selection circuitry is disclosed (figure 4, "punch in account designation").

Regarding claim 47, recall circuitry is disclosed (figure 4, "pin number").

Regarding claim 48, a display is disclosed (figure 1, numeral 15).

Differences:

While McIntosh uniquely associates a user-entered random password with a respective one of the indicia, and while McIntosh teaches a random number generator for purposes other than generating actual passwords (i.e., "unit 55 capable of generating a random sequence of numbers when required" at page 3, line 14), McIntosh does not disclose "password circuitry comprising a random number generator for randomly generating a plurality of passwords".

Art Unit: 2621

Noll et al.:

Noll discloses a system for generating a password, wherein Noll teaches random number generator ("generating a random number" at column 1, line 49; "creating a sequence of random numbers" at column 4, line 12) for randomly generating a password ("passwords" at column 1, line 23) for a use to gain access to a system ("security system" at column 1, line 48).

Obviousness Statement:

It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the password circuitry of McIntosh according to the teaching of Noll, by including a random number generator to generate random passwords/PINs for the user for purposes of gaining access to his/her secure accounts so that when it comes time for the user to either choose a password, or to change a password, the password can be randomly generated. The addition of a random password generator as taught by Noll would serve to provide a "completely random password" which "presents no opening or prior knowledge that can be exploited by an hostile agent" (Noll, column 1, line 50).

Art Unit: 2621

14. Claims 45-48 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and PassMan™ (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm))<sup>1</sup>.

#### McIntosh in view of PassMan

##### McIntosh:

Regarding claims 45 and equivalent claim 53, McIntosh discloses:

a portable body member (figure 1, numeral 5);

a data storage in the body (figure 2, numeral 40);

a user interface and communication components (figure 1, numerals 10, 15, 20 and 25) permitting an individual to store plural indicia representative of a secure site in the storage ("letters" at page 2, line 44; e.g., "BC" at page 3, line 39); and

password circuitry for allowing a user enter a plurality of passwords, wherein each password is uniquely associated with a respective one of the indicia ("sequence of numbers" at page 2, line 45; e.g., "1234" at page 3, line 42; in the example given by McIntosh at page 3, lines 25-44, the indicia "BC" is uniquely associated with the password "1234"; the input keys, along with their control circuitry and the memory 40, is circuitry that allows for the generation of passwords by a user).

---

<sup>1</sup> Archived on April 8, 1999 by the Wayback Machine at [www.archive.org](http://www.archive.org); Note: The pages have been numbered by the examiner as 1-13, with page 1 corresponding to the search result for [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm), pages 2-3 being the webpage itself, pages 4-7 being the source code for the webpage, pages 8-11 being the link for "Screenshots" from page 2, and pages 12-13 being the link for "ZDNet Review" from page 2.

Art Unit: 2621

Regarding claim 53 specifically, the steps of associating a password with an indicia can be repeated by a user as many times as desired as permitted by the memory capacity of the memory device (“... entered and recorded in like manner if so desired” at page 4, line 1).

Regarding claim 46, indicia selection circuitry is disclosed (figure 4, “punch in account designation”).

Regarding claim 47, recall circuitry is disclosed (figure 4, “pin number”).

Regarding claim 48, a display is disclosed (figure 1, numeral 15).

Differences:

While McIntosh uniquely associates a user-entered password with a respective one of the indicia, and while McIntosh teaches a random number generator for purposes other than generating actual passwords (i.e., “unit 55 capable of generating a random sequence of numbers when required” at page 3, line 14), McIntosh does not disclose “password circuitry comprising a random number generator for randomly generating a plurality of passwords” for the association as required by claim 45 in step d, and claim 53 in step c.

PassMan:

PassMan discloses a software system which runs on a general purpose computer, in the exact same field of password storage (“Password List Manager” at page 2), where PassMan associates a user entered indicia with its corresponding

Art Unit: 2621

password ("Password List" at page 8), comprising a random number generator ("generates random alphanumeric passwords" at page 2; see the "Generate Random Password" button at page 8) for randomly generating a plurality of passwords (the user can generate a random password for each account name stored as depicted on page 8) for the association with the indicia (as depicted on page 8, each "user name" which is an indicia is associated with a "Password/Code").

Obviousness Statement:

It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the circuitry/programming of the McIntosh portable password storage device, by adding a random password generator for purposes of associating a random password with an indicia as taught by PassMan, so that the user does not "have to hassle with it" (PassMan, page 2), and so that the user can generate passwords that are more secure, and less prone to attack by hacking, because they are in fact completely random and for simple convenience (this is "knowledge generally available to one of ordinary skill in the art" as stated by MPEP 2143.01; while not part of this grounds of rejection, evidence of this can be found by the statements of the He reference and Noll reference above; e.g. Noll states that a "completely random password ... presents no opening or prior knowledge that can be exploited by an hostile agent" at column 1, line 50; the He reference states that a random password may "increase the security level due to the unpredictability of the password" at column 8, line

Art Unit: 2621

1, and that a randomly generated password provides “for convenience and for uniqueness” at column 13, line 6)

Alternate Rejection: PassMan in view of McIntosh:

PassMan:

Regarding claims 45 and equivalent claim 53, PassMan discloses:

a computer (the PassMan system is a software system that runs on a computer programmed with the software; thus, PassMan teaches an apparatus);

a data storage in the body (the computer, once programmed by PassMan, stores indicia and passwords);

a user interface and communication components (the programmed computer has a user interface, as shown on pages 8-11) permitting an individual to store plural indicia representative of a secure site in the storage (“UserName” at page 8); and

password circuitry comprising a random number generator for randomly generating a plurality of passwords (“generates random alphanumeric passwords” at page 2; see the “Generate Random Password” button at page 8), where each of the passwords is uniquely associated with a respective one of the indicia (as depicted on page 8, each “user name” which is an indicia is associated with a “Password/Code”).

Regarding claim 53 specifically, the steps of associating a password with an indicia can be repeated by a user as many times as desired as permitted by the memory capacity of the memory device (as depicted on page 8, a plurality of indicia and passwords may be stored)



Art Unit: 2621

Regarding claim 46-48, indicia selection circuitry, recall circuitry and a display is disclosed (page 8).

Differences:

PassMan does not teach the system being embodied in a **portable body member**.

McIntosh:

McIntosh discloses a system for storing and associating indicia with passwords, comprising a portable body member (figure 1, numeral 5).

Obviousness Statement:

It would have been obvious at the time the invention was made to one of ordinary skill in the art to embody the computer software/hardware system of PassMan, in a portable body member as taught by McIntosh, in order to provide the capabilities of PassMan (i.e., password recall) in a "pocket-sized" device (McIntosh, page 1, line 26) having "substantially the same size and shape as a standard bank/credit card" (McIntosh, page 1, line 35), thereby allowing the user to conveniently carry the device with him for recalling, at remote locations (e.g., an ATM machine) a required password.

Art Unit: 2621

15. Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and PassMan™ (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) as applied to claim 47 above, and further in view of Bang (US 6,088,143 A).

The McIntosh and PassMan combination does not teach a communication port on the portable device for directly transmitting the password(s) to the secure site(s).

Bang teaches a remote password key system ("infrared password key system" at column 1, line 19) comprising a communication port ("infrared transmitter" at column 3, line 29) for directly transmitting a password ("the password signal directed for direct transmittal" at column 3, line 31) to a secure site ("transmitting ... to the computer" at column 3, line 33).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to provide the portable device of the McIntosh and PassMan combination, with a direct password transmission port as taught by Bang, in order to "simplify the computer password input procedure and to reduce the possibility of unintentional password disclosure to a third party when entering a password" (Bang, column 1, line 20).

Art Unit: 2621

16. Claims 50-52 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and PassMan™ (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) as applied to claim 45 above, and further in view of Guthrie et al. (US 6,161,185 A).

Regarding claim 50, the McIntosh and PassMan combination does not teach prompting the user to change a password after expiration of a predetermined period of time.

Regarding claim 51, the combination does not teach clock circuitry and circuitry to display a message requiring the individual to reply to continue using the device.

Regarding claim 50, Guthrie discloses a personal authentication system comprising prompting the user to change a password ("requiring users to change their passwords" and "sufficient notice" at column 2, lines 35 and 36) after expiration of a predetermined period of time ("expire after a predetermined period of time" at column 2, line 34).

Regarding claim 51, Guthrie teaches clock circuitry (i.e., the circuitry that keeps track of the time period as described above) and circuitry to display a message requiring the individual to reply (i.e., the aforementioned circuitry that provides "sufficient notice") to continue using the device ("locked out" at column 2, line 39).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the McIntosh and PassMan combination, to notify and require the user to change passwords associated with the indicia after predetermined periods of time, in order to "foil a malicious user's attempt at 'hammering' the authentication

Art Unit: 2621

system with responses attempting to stumble upon a correct password to gain access” (Guthrie, column 2, line 53).

Regarding claim 51, the combination does not teach generating a new password when the prompt is actuated. However, in the above McIntosh, PassMan and Guthrie combination, it would have been obvious to allow the user to change his password in response to the prompt taught by Guthrie, by randomly generating another password in accordance with the McIntosh and PassMan combination, so as to ensure that the user is not locked out.

Regarding claim 54, the limitations therein are met by the McIntosh, PassMan and Guthrie combination as described above.

17. Claims 33-36, 38, 39, 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A) and PassMan<sup>TM</sup> (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) as applied to claim 45-48 and 53 above, and further in view of Ramachandran (US 6,315,195 B1).

The elements of claims 33-36, 38 and 39 (other than the differences discussed below) are met by the McIntosh and PassMan combination as described in the rejections above. Regarding claim 40 specifically, McIntosh teaches that a preselected string of predetermined length is stored (“first four letters” and “remaining two letters” at page 3, line 30).

The McIntosh and PassMan combination requires an initial password be entered for a user to gain access to the accounts and associated passwords stored therein (e.g.,

Art Unit: 2621

“the password” and “FLAG” at page 3, lines 32 and 33). The McIntosh and PassMan combination does not teach using biometrics for this same purpose. Specifically, the combination does not teach a biometric interface engaged with the body, a non-volatile memory, generating and storing an initialized biometric template and comparing with a second generated biometric template upon subsequent presentation for enabling the device.

Ramachandran discloses a portable device (e.g., figures 1 and 2) for storing pin numbers (e.g., figures 82+) as described fully in the previous Office Action, comprising biometric interface engaged with the body (figure 4, numeral 47), a non-volatile memory (figure 4, numeral 38), generating and storing an initialized biometric template (“data representative of the identifying biometric features” at column 8, line 59) and comparing with a second generated biometric template upon subsequent presentation (“compare” at column 12, line 24) for enabling the device (“enable authorized users of the card” at column 8, line 61). Regarding claim 39 specifically, a fingerprint reader is disclosed (“fingerprint” at column 8, line 53).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to replace the initial password circuitry of the McIntosh and PassMan combination, with biometrics comparison circuitry as taught by Ramachandran as described above, in order to “increase the security level” (Ramachandran, column 11, line 8) thus providing increased protection from an unauthorized user from gaining access to the legitimate user’s passwords.

Regarding claim 41, while the McIntosh and PassMan combination teaches a plurality of function keys on the portable device (i.e., McIntosh, figure 1, numeral 10), arrow keys are not disclosed. However, McIntosh states that "a more complex version of the device 5 might well be produced incorporating ... more function keys" at page 4, line 33. Ramachandran discloses arrow keys (figure 1, numerals 4 and 26) for purposes of scrolling up and down through a data list. It would have been obvious at the time the invention was made to one of ordinary skill in the art to provide the arrow keys of Ramachandran, on the device of the McIntosh and PassMan combination, to increase functionality as suggested by McIntosh, and to allow a user to scroll through a list of data without having to re-enter the initial password each time.

18. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A), PassMan™ (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) and Ramachandran (US 6,315,195 B1) as applied to claim 35 above, and further in view of Bang (US 6,088,143 A).

The McIntosh, PassMan and Ramachandran combination does not teach a communication port on the portable device for directly transmitting the password(s) to the secure site(s).

Bang teaches a remote password key system ("infrared password key system" at column 1, line 19) comprising a communication port ("infrared transmitter" at column 3, line 29) for directly transmitting a password ("the password signal directed for direct

Art Unit: 2621

transmittal" at column 3, line 31) to a secure site ("transmitting ... to the computer" at column 3, line 33).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to provide the portable device of the McIntosh, PassMan and Ramachandran combination, with a direct password transmission port as taught by Bang, in order to "simplify the computer password input procedure and to reduce the possibility of unintentional password disclosure to a third party when entering a password" (Bang, column 1, line 20).

19. Claims 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McIntosh (GB 2,274,184 A), PassMan<sup>TM</sup> (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) and Ramachandran (US 6,315,195 B1) as applied to claim 33 above, and further in view of Guthrie et al. (US 6,161,185 A).

Regarding claim 42, the McIntosh, PassMan and Ramachandran combination does not teach prompting the user to change a password after expiration of a predetermined period of time.

Regarding claim 43, the combination does not teach clock circuitry and circuitry to display a message requiring the individual to reply to continue using the device.

Regarding claim 42, Guthrie discloses a personal authentication system comprising prompting the user to change a password ("requiring users to change their passwords" and "sufficient notice" at column 2, lines 35 and 36) after expiration of a

Art Unit: 2621

predetermined period of time ("expire after a predetermined period of time" at column 2, line 34).

Regarding claim 43, Guthrie teaches clock circuitry (i.e., the circuitry that keeps track of the time period as described above) and circuitry to display a message requiring the individual to reply (i.e., the aforementioned circuitry that provides "sufficient notice") to continue using the device ("locked out" at column 2, line 39).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the McIntosh, PassMan and Ramachandran combination, to notify and require the user to change passwords associated with the indicia after predetermined periods of time, in order to "foil a malicious user's attempt at 'hammering' the authentication system with responses attempting to stumble upon a correct password to gain access" (Guthrie, column 2, line 53).

Regarding claim 44, the combination does not teach generating a new password when the prompt is actuated. However, in the above McIntosh, PassMan, Ramachandran and Guthrie combination, it would have been obvious to allow the user to change his password in response to the prompt taught by Guthrie, by randomly generating another password in accordance with the McIntosh and PassMan combination, so as to ensure that the user is not locked out.



Art Unit: 2621

20. Claims 45-48 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of PassMan™ (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) and Notebooks.com (archive website [www.notebooks.com](http://www.notebooks.com))<sup>2</sup>.

PassMan:

Regarding claims 45 and equivalent claim 53, PassMan discloses:

a computer (the PassMan system is a software system that runs on a computer programmed with the software; thus, PassMan teaches an apparatus);

a data storage in the body (the computer, once programmed by PassMan, stores indicia and passwords);

a user interface and communication components (the programmed computer has a user interface, as shown on pages 8-11) permitting an individual to store plural indicia representative of a secure site in the storage ("UserName" at page 8); and

password circuitry comprising a random number generator for randomly generating a plurality of passwords ("generates random alphanumeric passwords" at page 2; see the "Generate Random Password" button at page 8), where each of the passwords is uniquely associated with a respective one of the indicia (as depicted on page 8, each "user name" which is an indicia is associated with a "Password/Code").

---

<sup>2</sup> Archived on December 22, 1996 by the Wayback Machine at [www.archive.org](http://www.archive.org); Note: The pages have been numbered by the examiner as 1-34, with page 1 corresponding to the search result for [www.notebooks.com](http://www.notebooks.com), pages 2-4 being the webpage itself, pages 5-10 being the source code for the webpage, pages 11-12 being the link for "COMPAQ" from page 2, and pages 13-25 being the link for "COMPAQ", pages 26-29 being the link "Armada 4130" from page 11, with pages 30-34 being its source code.

Art Unit: 2621

Regarding claim 53 specifically, the steps of associating a password with an indicia can be repeated by a user as many times as desired as permitted by the memory capacity of the memory device (as depicted on page 8, a plurality of indicia and passwords may be stored)

Regarding claim 46-48, indicia selection circuitry, recall circuitry and a display is disclosed (page 8).

Differences:

While PassMan is software that operates on personal computers that runs Windows 95 or 98 ("Windows95/98" at PassMan page 2), and while Window 95 and 98 were both commonly used to operate laptop and notebook computers well before the time the invention was made, and while PassMan can and was most certainly used on laptop and notebook computers, PassMan does not EXPLICITLY disclosed the system being embodied in a **portable body member**.

Notebooks.com

Notebooks.com teaches a notebook computer ("Compaq Armada 4130T" at page 11, and pages 26-29), comprising a portable body member ("Dimensions" and "Weight" at page 27; the dimensions of the standard configuration are 1.5 X 11.6 X 10.3 inches, and the weight is 6 pounds; this constitutes a portable body member) that operates using the Windows 95 software ("Software" and "Windows 95" at page 28).

Art Unit: 2621

Obviousness Statement:

It would have been obvious at the time the invention was made to one of ordinary skill in the art to embody/utilize the software of PassMan, in a portable body member (i.e., a notebook computer) as taught by Notebooks.com, by simply loading the software of PassMan onto the portable body (i.e., notebook computer) thereby programming the circuitry of the portable body member to perform the functions of PassMan, in order to provide the capabilities of PassMan (i.e., password recall) on a portable computing device so that the user may recall passwords anywhere, or anytime he or she has the notebook with them such as at work, on vacation, etc., thereby providing convenient, rapid access to the user's password anywhere (i.e., for the same, well known reasons that notebook computers became popular in the first place).

21. Claims 33 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of PassMan<sup>TM</sup> (archived website [www.ijen.net/passman.htm](http://www.ijen.net/passman.htm)) and Notebooks.com (archive website [www.notebooks.com](http://www.notebooks.com)) as applied to claim 45-48 and 53 above, and further in view of Ramachandran (US 6,315,195 B1).

The PassMan and Notebooks.com combination requires that an initial question to be answered (i.e., an initial password be entered) for a user to gain access to the accounts and associated passwords stored therein ("Set Question" and "Set Answer" at PassMan page 10). The combination does not teach using biometrics for this same purpose. Specifically, the combination does not teach a biometric interface engaged with the body, a non-volatile memory, generating and storing an initialized biometric

Art Unit: 2621

template and comparing with a second generated biometric template upon subsequent presentation for enabling the device.

Ramachandran discloses a portable device (e.g., figures 1 and 2) for storing pin numbers (e.g., figures 82+) as described fully in the previous Office Action, comprising biometric interface engaged with the body (figure 4, numeral 47), a non-volatile memory (figure 4, numeral 38), generating and storing an initialized biometric template ("data representative of the identifying biometric features" at column 8, line 59) and comparing with a second generated biometric template upon subsequent presentation ("compare" at column 12, line 24) for enabling the device ("enable authorized users of the card" at column 8, line 61). Regarding claim 39 specifically, a fingerprint reader is disclosed ("fingerprint" at column 8, line 53).

It would have been obvious at the time the invention was made to one of ordinary skill in the art to replace or supplement the initial question/password circuitry of the PassMan and Notebooks.com combination, with biometrics comparison circuitry as taught by Ramachandran as described above, in order to "increase the security level" (Ramachandran, column 11, line 8) thus providing increased protection from an unauthorized user from gaining access to the legitimate user's passwords.

### ***Conclusion***

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

PassGen (archived website <http://www.world.std.com/~reinhold/passgen.html>)<sup>3</sup> is extremely pertinent as teaching a random number generator for generating randomized passwords for a user, as well as motivation and reasoning as to why someone would want to generate randomized passwords (i.e., page 2).

WebConfidential (archived website <http://web-confidential.com>)<sup>4</sup> is extremely pertinent as teaching software system for organizing and associating a user's passwords and indicia indicative of accounts (pages 1 and 16).

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian P. Werner whose telephone number is 703-306-3037. The examiner can normally be reached on M-F, 8:00 - 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Leo H. Boudreau can be reached on 703-305-4706. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9314 for regular communications and 703-872-9314 for After Final communications.

---

<sup>3</sup> Archived on May 8, 1999 by the Wayback Machine at [www.archive.org](http://www.archive.org); Note: The pages have been numbered by the examiner as 1-8.

<sup>4</sup> Archived on December 12, 1998 by the Wayback Machine at [www.archive.org](http://www.archive.org); Note: The pages have been numbered by the examiner as 1-51.

Art Unit: 2621

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-4750.

Brian Werner  
Primary Examiner  
July 2, 2003

A handwritten signature in black ink, consisting of a large, stylized 'B' followed by a series of loops and a long horizontal stroke extending to the right.

**BRIAN WERNER  
PRIMARY EXAMINER**